

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA**

UNITED STATES OF AMERICA,

Plaintiff,

vs.

MARK RINGLAND,

Defendant.

8:17CR289

MEMORANDUM AND ORDER

This matter is before the Court on the Findings and Recommendation (F&R), ECF No. 74, issued by Magistrate Judge Michael D. Nelson, recommending that the Motion to Suppress, ECF No. 47, and Motion to Suppress and Application for *Franks* Hearing, ECF No. 49, filed by the Defendant, Mark Ringland, be denied. Ringland filed an Objection to the Findings and Recommendation and a brief in support, ECF No. 75, as allowed by 28 U.S.C. § 636(b)(1)(C) and NECrImR 59.2(a). The Government did not respond to the Objection. For the reasons set forth below, the F&R will be adopted and the Motion to Suppress will be denied.

BACKGROUND

Defendant is charged with receipt of child pornography and possession of child pornography. Indictment, ECF No. 20. Ringland does not object to the Magistrate Judge's findings of fact included in the F&R, but objects to the Magistrate Judge's failure to include each and every fact contained in Ringland's Supplemental Brief, ECF No. 70 at 2-24. The Court has reviewed the record and each of the facts listed in Ringland's briefs, and concludes that the Magistrate Judge did not err in failing to restate every fact listed in Ringland's briefs. Several of Ringland's asserted facts are descriptions of the

law, legal argument, or legal conclusions. Each of the facts stated by the Magistrate Judge is supported by the record. To the extent certain facts were omitted, the F&R demonstrates that the Magistrate Judge considered all the evidence and did not omit any material facts.

The Court adopts the Magistrate Judge's factual findings in their entirety and provides the following by way of summary.

Investigator C.J. Alberico of the Nebraska State Patrol investigated Ringland's conduct, leading to the charges filed in this case. TR.¹ 55; D.E.² 163. According to Alberico, Google, Inc. (Google) first provided information to the National Center for Missing and Exploited Children (NCMEC) that a user of Google's services "had uploaded over seven hundred (700) files suspected of depicting sexually explicit conduct involving a minor." D.E. 109 at 7. Google identified the user by email address, mringland69@gmail.com, with associated telephone number 402-***-0642. Several IP addresses were associated with the uploaded files, which NCMEC traced to Sprint PCS in Omaha, Nebraska. Based on this information, on April 17, 2017, NCMEC created seven CyberTipline reports: #19083866, #19153972, #19938982, #19986242, #20035870, #20260729, and #20293287. D.E. 163 at 1.

Deputy Mark Dishaw, of the Douglas County, Nebraska, Sheriff's Office, testified that an electronic service provider ("ESP"), such as Google, has proprietary methods to filter and identify known child pornography images based on hash values. TR. 21-22, 24-25, 51-53. The ESP then views the file images and reports potential violations to NCMEC

¹ References to "TR" are to the Transcript of the evidentiary hearing at ECF No. 68.

² References to G.E. and D.E. are to Government's Exhibit and Defendant's Exhibit, respectively.

which generates CyberTipline reports to send to law enforcement. TR. 14-16. Law enforcement then reviews the files identified by the ESP.

On June 23, 2017, Alberico received CyberTipline Report #20437297, which Google previously submitted to NCMEC. On June 27, 2017, Alberico prepared a Douglas County search warrant affidavit, search warrant, and non-disclosure order for the email account mringland69@gmail.com, associated with telephone number 402-***-0642. D.E. 163 at 1-2; D.E. 109-110. Alberico stated in her affidavit supporting the application that Google “reviewed five hundred and two (502) files from the CyberTips submitted” and that she “only viewed files that were reviewed by Google . . . to confirm they depicted child pornography.” D.E. 109 at 7. Alberico obtained a warrant to search the account.

Alberico observed that email address mringland69@gmail.com had sent child erotica photographs and images of child pornography to the email address mringland65@gmail.com. D.E. 163 at 2. On July 19, 2017, Alberico received CyberTipline reports #21681475 and #22346425. These reports listed the email address markringland65@gmail.com, with associated telephone 402-***-0902, and a secondary email address, mringland69@gmail.com. NCMEC traced several of the IP addresses associated with the uploaded files to Sprint PCS in the Omaha area, and Google provided the name “Mark Ringland” associated with the two email addresses. D.E. 163 at 2. Pursuant to a subpoena served by Alberico on July 20, 2017, Sprint PCS identified the subscriber of telephone number 402-***-0902 as Mark Ringland, residing at 1904 Pleasantview Ln, Bellevue, Nebraska 68005.

On August 7, 2017, Alberico received nine more CyberTipline reports: #22968026, #22968382, #22968534, #23001904, #23002061, #2302151, #23002255, #23043174,

and #23043630, all of which were associated with the email address markringland65@gmail.com. On the same date, Alberico prepared a Douglas County search warrant affidavit, search warrant, and non-disclosure order for the email accounts mringland65@gmail.com and markringland65@gmail.com, associated with telephone number 402-***-0902. D.E. 122-123.

On August 14, 2017, Alberico received five additional CyberTipline reports, #23245909, #23274478, #23249764, #23249764 and #23068622, and on August 25, 2017, six more, #23411893, #23488795, #23512952, #23545730, #23588762, and #233890937. All the reports were associated with email addresses markringland65@gmail.com and mringland69@gmail.com, and the telephone number 402-***-0902. D.E. 163 at 4.

On August 18, 2017, Alberico received information from Google pursuant to the previous search warrant. Alberico reviewed files from Google and concluded that several of the files contained images and/or videos of suspected child pornography and bestiality. D.E. 124 at 10. Based on that information, Alberico applied for a United States District Court search and seizure warrant affidavit, search warrant, and non-disclosure order for a cellular ping order for telephone number 402-***-0902, which was presented to and signed by a United States Magistrate Judge. D.E. 124-125; D.E. 163 at 4.

Alberico located Mark Ringland in the Nebraska Criminal Justice System (NCJIS), which indicated that a black Ford Windstar SE sport van with Nebraska license plate number UZP192 was registered to Ringland in June 2017, and that as of August 2017, the vehicle's registration address was 16406 Taylor Street, Omaha, NE 68116. Nebraska Department of Labor records indicated that Ringland was employed by Merrick Machine

Company, located in Alda, Nebraska, and by the temporary agency Essential Personnel Inc., based out of Grand Island Nebraska, with hub offices in Kearney, Nebraska and Denver, Colorado. D.E.163 at 3.

On September 1, 2017, Alberico obtained a United States District Court search warrant for Ringland's person and cellular telephone, phone number 402-***-0902, D.E. 126-127, and a criminal complaint and arrest warrant. On the same date, law enforcement executed a search warrant at 16406 Taylor Street in Omaha, and arrested Ringland pursuant to the warrant. Ringland was read his *Miranda* rights, which he waived, and consented to an interview. D.E. 163 at 4. Alberico indicated in her report that on September 5, 2017, Ringland made spontaneous statements to the United States Marshals transporting him for his initial hearing. D.E. 163 at 4-5.

Ringland seeks to suppress all evidence seized in connection with the searches of his email accounts, and any incriminatory statements made after his arrest and during transportation to his initial appearance. Ringland argues that Google acted as a government agent when it searched his emails without a warrant and forwarded those contents to NCMEC; that NCMEC expanded upon Google's warrantless searches; and that the warrants obtained by Alberico were supported in substantial part by such warrantless searches. Ringland also seeks a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), arguing that the applications supporting the warrants in this case omitted information material to the probable cause determination. The Magistrate Judge recommends that both motions be denied. Ringland objects to the Magistrate Judge's conclusions. Although Ringland asserts twelve different objections, many of them overlap and each is addressed below.

STANDARD OF REVIEW

Under 28 U.S.C. § 636(b)(1)(C) and NECrimR 59.2(a), the Court shall make a *de novo* review of the portions of the Magistrate's Findings and Recommendation to which objections have been made. The Court may accept, reject, or modify, in whole or in part, the Magistrate Judge's findings and recommendations. The Court may also receive further evidence or remand the matter to the Magistrate Judge with instructions.

DISCUSSION

I. Franks Hearing

Affidavits supporting a search warrant are presumed valid. *Franks v. Delaware*, 438 U.S. 154, 171 (1978). "Under *Franks*, a criminal defendant may request a hearing to challenge a search warrant on the ground that the supporting affidavit contains factual misrepresentations or omissions relevant to the probable cause determination." *United States v. Arnold*, 725 F.3d 896, 898 (8th Cir. 2013). To meet the burden of demonstrating that such a hearing is warranted, the defendant must make "a substantial preliminary showing." *Franks*, 438 U.S. at 155. The defendant must demonstrate that the affidavit supporting the warrant "contained false statements or omissions that were material to the finding of probable cause," *United States v. Oleson*, 310 F.3d 1085, 1090 (8th Cir. 2002). "The type of showing required is not easily met." *United States v. Gabrio*, 295 F.3d 880, 883 (8th Cir. 2002).

Ringland argues that he is entitled to a *Franks* hearing because Alberico did not include in her warrant applications that there were other geographic locations and internet protocol (IP) addresses associated with images outlined in the NCMEC CyberTipline reports. Ringland also argues that he is entitled to a *Franks* hearing because only a small

portion of the files was categorized as “apparent child pornography.” Finally, Ringland argues that Google and NCMEC were state actors for purposes of the Fourth Amendment and therefore their warrantless searches of his personal email and phone numbers were unconstitutional. Upon review of the record, none of these arguments entitles Ringland to a *Franks* hearing.

A. IP Addresses and Geographic Locations

It is undisputed that Alberico did not include information about other IP addresses contained in the NCMEC CyberTipline reports in the affidavit. Yet information in the affidavit related to Ringland’s identity was sufficient to support a probable cause finding. The record demonstrates that the CyberTipline reports identified email addresses and a phone number connected to Ringland. For example, the first application stated that the tips were related to the email address markringland69@gmail.com and phone number 402-xxx-0642. The second warrant application identified markringland65@gmail.com and mringland69@gmail.com, as well as the phone number 402-xxx-0902. Based on the information obtained from the first two warrants and independent investigation, investigators obtained a ping warrant that led them to Ringland’s geographic location. The issuing judge reasonably relied on information about the phone number repeatedly appearing in reports to issue the ping warrant that identified Ringland’s precise geographic location, regardless of the IP addresses or geographic locations associated with them. The omission of information regarding additional IP addresses did not diminish the evidence supporting probable cause. Accordingly, the Court adopts the Magistrate Judge’s conclusion.

B. Categorization of Files as Apparent Child Pornography

Each report from NCMEC contains an executive summary that describes the total number of uploaded files sent by Google and contains NCMEC's categorization of the material contained in those files, e.g., "Apparent Child Pornography" or "Uncategorized." D.E. 101-108; 112-121; & 128-143. Ringland notes throughout his briefing that the great majority of the files were deemed "uncategorized," and the Court infers that he suggests such files did not contain child pornography and the omission of this fact from the application was misleading.³

Dishaw's testimony demonstrated that the "uncategorized" label was not an indication that a file contained no child pornography. Rather, the files that were categorized as potentially containing child pornography were ones that had been flagged by hash values. TR. 52. Files that were "uncategorized" were not tagged by hash values but were identified as containing child pornography through some other method. *Id.* In Alberico's application, she stated that she reviewed 502 image files identified and viewed by Google, and confirmed they depicted child pornography. Thus, even though the files were labeled as "uncategorized" in the NCMEC executive summary, there is evidence that they contained child pornography.

C. Google and NCMEC as State Actors

Ringland argues that Google and NCMEC were state actors and conducted an illegal search under the Fourth Amendment. This argument is the principal basis for Ringland's motion to suppress. For the reasons stated below, the Court cannot conclude that Google or NCMEC conducted an illegal search or that Alberico impermissibly

³ Ringland never expressly describes his argument with respect to the uncategorized files.

examined the files prior to requesting a warrant. Accordingly, Ringland is not entitled to a *Franks* hearing on that basis.

II. Motion to Suppress

Ringland argues that his Fourth Amendment rights were violated when Google and NCMEC searched his email accounts without a warrant. Ringland argues that Google was a government actor because its purpose was to help law enforcement and the government knew Google was searching Ringland's emails. Ringland also argues that NCMEC impermissibly expanded the scope of Google's search.

The Fourth Amendment demands that people shall "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, . . . and no Warrants shall issue, but upon probable cause. . . ." U.S. Const., amend. IV. "The Fourth Amendment applies only to state action, so it does not constrain private parties unless they act as agents or instruments of the government." *United States v. Stevenson*, 727 F.3d 826, 829 (8th Cir. 2013) (citing *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). For purposes of the Fourth Amendment, private parties act as agents of the government when "a statute or regulation compels a private party to conduct a search" or "a statute or regulation so strongly encourages a private party to conduct a search that the search is not primarily the result of private initiative." *Id.* (internal quotation marks and citation omitted).

The statutes at issue in this case do not compel or "strongly encourage" disclosure of private information. The Stored Communications Act, 18 U.S.C. § 2701, generally prohibits computing service providers from disclosing contents of accounts except under specific, enumerated circumstances. Section 2702(b)(6) provides that service providers

may “divulge the contents of a communication . . . to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A.” Section 2258A requires service providers to report to the NCMEC any apparent violation of the child pornography laws discovered while providing electronic communication services. *Stevenson*, 727 F.3d at 829 (citing 18 U.S.C. § 2258A(a)).

The Eighth Circuit has held that the reporting requirement of § 2258A, standing alone, “does not transform an [i]nternet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography.” *Id.* at 831. Instead, courts must consider several factors to determine whether a private party acts as an instrument of the government. See *id.* at 830 (citing *United States v. Smith*, 383 F.3d 700, 705 (8th Cir. 2004)). These factors include “(1) whether the government had knowledge of and acquiesced in the intrusive conduct;” (2) “whether the citizen intended to assist law enforcement agents or instead acted to further his own purposes;” and (3) “whether the citizen acted at the government’s request.” *Smith*, 383 F.3d at 705. Applying these factors to Google and NCMEC, the Magistrate Judge correctly concluded that these entities were not government actors for purposes of the Fourth Amendment.

A. Google

There is no evidence that Google searched Ringland’s email accounts at the Government’s request. Ringland argues that the § 2258A’s statutory scheme nevertheless “strongly encouraged” the search. However, the Eighth Circuit has held that § 2258A’s reporting requirements are not sufficient on their own to make Google a government actor. *Stevenson*, 727 F.3d at 831.

There is also no evidence that Google acted with intent to assist government agents rather than to further its own purposes. Cathy McGoff, Senior Manager, Law Enforcement and Information Security at Google, stated Google's terms of service prohibit using Google's services in violation of law. McGoff Decl., ECF No. 73-2 at 1. The terms of service also provide that Google "may review content to determine whether it is illegal or violates our policies, and we may remove or refuse to display content that we reasonably believe violates our policies or the law." *Id.* at 1-2. McGoff explained that Google has a "strong business interest in enforcing our terms of service and ensuring that our services are free of illegal content, including in particular child sexual abuse material." *Id.* at 2. For this reason, Google "independently and voluntarily take[s] steps to monitor and safeguard our services against this content because users will stop using our services if they become associated with being a haven for abusive content." *Id.* Google discovered the images using its own hash values and reviewers, and the searches furthered Google's own business interests. *Id.* at 3. Forwarding the images to NCMEC consistent with § 2258A did not make Google a government actor, nor does it indicate that Google acted with intent to aid law enforcement.

Ringland argues that Google's intent to aid law enforcement is demonstrated by its accelerated investigatory efforts after the initial report to NCMEC and the fact that Google connected Ringland's two email addresses. Ringland argues that "protracted, independent investigatory acts suggest that Google remained an active participant in this investigation well beyond the initial CyberTips." Yet Ringland cites no authority to support his theory that once a private actor becomes aware of potentially illegal conduct it must cease further investigation. After Google became aware of potential issues with

Ringland's accounts, it reasonably investigated to determine whether there were other potential violations of the terms of service. These actions furthered Google's legitimate business interests and Google did not violate the Fourth Amendment by fulfilling its reporting requirements under § 2258A.

Finally, there is no evidence that the government knew of or acquiesced to Google's conduct, giving rise to any violation the Fourth Amendment. As the Magistrate Judge noted, "voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent." F&R, ECF No. 74 at 10 (quoting *Stevenson*, 727 F.3d at 831). Although Google actively investigated and reported information about Ringland's accounts, there is no evidence that it did so at the request of government officials.

B. NCMEC

Ringland argues that even if Google was not a government actor, NCMEC violated the Fourth Amendment when it expanded the searches initiated by Google. The Eighth Circuit has not addressed this subject, but other circuits have. The Tenth Circuit concluded that NCMEC is a government agent when it expands upon the scope of a service provider's investigation without a warrant. See *United States v. Ackerman*, 831 F.3d 1292, 1306–07 (10th Cir. 2016). Conversely, where the NCMEC only views files flagged as containing child pornography, it does not violate the Fourth Amendment. *United States v. Reddick*, 900 F.3d 636, 639–40 (5th Cir. 2018). The Magistrate Judge concluded there was no evidence that NCMEC viewed more files than those reviewed by Google. Ringland "strenuously objects" to the Magistrate Judge's conclusion, arguing that NCMEC viewed several files that Google had not. See F&R, ECF No. 74 at 10.

In Alberico's affidavit supporting her initial warrant application, she stated that Google reviewed 502 of the 1,216 files submitted to NCMEC. See D.E. 109 at 7. The Magistrate Judge concluded that this case is like *Reddick* because Alberico stated she only reviewed those 502 files. Ringland objects to this conclusion because the executive summary of initial CyberTip reports refers to "over 700 uploaded files." D.E. 109 at 1. The Court infers that Ringland argues this case is more like *Ackerman* because NCMEC admitted it reviewed more files than Google reviewed.

The affidavit supporting the initial warrant relied on Google's and Alberico's review of the same files. Alberico acknowledged that the initial CyberTip reports included 1,216 files, but she affirmed that she viewed only the files already reviewed by Google. Thus, even if NCMEC viewed more than 502 files, the initial application relied only on the 502 files already reviewed by Google.

Ringland does not explain how NCMEC's review could have tainted the application. John Shehan,⁴ Vice President of the Exploited Children Division of the NCMEC, testified that NCMEC is not required to review any files, and that it does so in furtherance of its private mission to aid children. G.E. 1 at 4. Shehan testified that after compiling CyberTipline reports, NCMEC forwards them to law enforcement for review. *Id.* at 5. Although CyberTipline reports triggered an investigation in this case, the application

⁴ Ringland objects to the Magistrate Judge's failure to find that Shehan's declaration was not credible. In support, Ringland offers Shehan's testimony in another case, *United States v. Miller*, No. CR 16-47-ART-CJS, 2017 WL 9325815 (E.D. Ky. May 19, 2017), *report and recommendation adopted*, No. CV 16-47-DLB-CJS, 2017 WL 2705963 (E.D. Ky. June 23, 2017), where Shehan failed to mention NCMEC's program that prevents NCMEC employees from reviewing files that had not been reviewed by the private service provider. Because NCMEC's program is not material to the Court's decision, the objection is overruled.

and ensuing warrant relied on Alberico's statement that she reviewed only files reviewed by Google. Accordingly, the Magistrate Judge's conclusion was not erroneous.

III. Good Faith

Ringland objects to the Magistrate Judge's conclusion that the good faith exception to the exclusionary rule applies to this case. Even where probable cause is lacking, an exception to the exclusionary rule applies where officers rely on a warrant in good faith. *United States v. Hessman*, 369 F.3d 1016, 1019 (8th Cir. 2004). In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court curtailed the use of the exclusionary rule as a remedy for unconstitutional searches and noted that the stated purpose of the exclusionary rule is "to deter *police* misconduct rather than to punish the errors of judges and magistrates." *Id.* at 916 (emphasis in original). "In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause." *Id.* at 920.

There is no allegation that the issuing judge wholly abandoned a detached and neutral role. Nor is there evidence that law enforcement officers were dishonest or misleading in preparing the Affidavit. Instead, Ringland argues that the good-faith exception does not apply in this case because the warrants were the product of illegal searches. For the reasons stated above, the Court concludes that the warrants were not illegal searches. Moreover, as addressed above, Albericio based her initial application on her own review of the files Google reviewed. Subsequent applications reasonably relied on information obtained under valid search warrants. Accordingly, the Magistrate Judge correctly concluded that the warrants were within the *Leon* good faith exception.

CONCLUSION

For the reasons discussed, the Findings and Recommendation will be adopted, and the Motions to Suppress and request for *Franks* hearing will be denied.

IT IS ORDERED:

1. The Findings and Recommendation, ECF No. 74, are adopted in their entirety;
2. The Motion to Suppress, ECF No. 47, and Motion to Suppress and Application for *Franks* Hearing, ECF No. 49, filed by the Defendant, Mark Ringland, are denied; and
3. The Objection to the Findings and Recommendation, ECF No. 75, is overruled.

Dated this 2nd day of January, 2019.

BY THE COURT:

s/Laurie Smith Camp
Senior United States District Judge